

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division

IN THE MATTER OF THE SEIZURE OF:	)	
	)	
ALL FUNDS IN TD BANK ACCOUNT	)	Case Nos.: 1:24-sw-608
NUMBER 4441040807 IN THE NAME	)	
OF CARSON TRUCK SERVICE INC.	)	
	)	
ALL FUNDS IN PNC BANK ACCOUNT	)	1:24-sw-609
NUMBER 53-6641-9861 IN THE NAME	)	
OF PHENIX BEAUTY SUPPLIES INC.;	)	
	)	
ALL FUNDS IN AN INTERNAL BANK	)	1:24-sw-610
OF AMERICA ACCOUNT HOLDING	)	
THE BALANCE OF ACCOUNT	)	
NUMBER 4350_4816_5747 IN THE	)	
NAME OF CHIA SUPPLIES CO	)	
LIMITED	)	
	)	

**AFFIDAVIT IN SUPPORT OF WARRANTS TO SEIZE PROPERTY SUBJECT TO  
FORFEITURE**

I, Samantha Wendt, being duly sworn, hereby, depose and state as follows:

**INTRODUCTION**

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been since June of 2023. I am currently assigned to the Washington Field Office. My primary duties include investigating violations of federal law, including securities fraud, wire fraud, bank fraud, and internet-enabled crimes. Part of those duties include investigating instances of wire fraud and bank fraud being used for financial gain at the expense of others. Before my career as an FBI Special Agent, I was employed as a Forensic Accountant by the FBI in the Seattle Field Office for two years. As part of that role, I conducted the financial portion of investigations, which

included reviewing financial records and determining the sources and uses of funds. I have participated in numerous investigations related to financial crimes and have experience analyzing financial documents, interviewing suspects and witnesses, and reviewing evidence obtained from physical and digital search warrants.

2. This affidavit is based on my personal investigation and the investigation of others, including federal and local law enforcement officials whom I know to be reliable. The facts and information contained in this affidavit are based upon witness interviews and my review of records, documents, and other physical evidence obtained during this investigation. This affidavit does not include each and every fact known to the government, but only those facts necessary to establish probable cause to support the issuance of the seizure warrant.

3. Based on the facts set forth in this affidavit, there is probable cause believe that the property set forth in the “Assets to be Seized” section of this affidavit are the proceeds of wire fraud, in violation of 18 U.S.C. § 1343, and mail fraud, in violation of 18 U.S.C. 1341. The proceeds of wire fraud and mail fraud are subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) and are subject to criminal forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) as incorporated by 28 U.S.C. § 2461(c).

**ASSETS TO BE SEIZED**

4. The assets to be seized are as follows (hereafter referred to as the “**SUBJECT ACCOUNTS**”):

- a. All funds in TD Bank Account #4441040807 (“**SUBJECT ACCOUNT 1**”), held in the name of Carson Truck Service Inc.;
- b. All funds in PNC Account #53-6641-9861 (“**SUBJECT ACCOUNT 2**”), held

in the name of Phenix Beauty Supplies Inc.; and

- c. Up to \$132,882.37 being held in an internal Bank of America Account holding the balance of Bank of America Account #4350\_4816\_5747 (“**SUBJECT ACCOUNT 3**”), held in the name of Chia Supplies Co Limited.

#### **LEGAL AUTHORITY**

5. 18 U.S.C. § 1341 (mail fraud) prohibits, in pertinent part, whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, by placing in an authorized depository for delivery by mail, by taking or receiving from an authorized depository for mail, by causing to be delivered by mail or by any private or commercial interstate carrier, and by depositing or causing to be deposited to be sent or delivered by any private or commercial interstate-carrier for the purpose of executing such scheme or artifice.

6. 18 U.S.C. § 1343 (wire fraud) prohibits, in pertinent part, whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, from transmitting or causing to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

7. 18 U.S.C. § 981(a)(1)(C) (forfeiture for specified unlawful activities) provides for the forfeiture of any property, real or personal, which constitutes or is derived from proceeds traceable to any offense constituting a specified unlawful activity (“SUA”), as defined in 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such SUA. 18 U.S.C. § 1956(c)(7)(A) provides that any

act or activity constituting an offense under 18 U.S.C. § 1961(1) constitutes an SUA, with the exception of an act indictable under subchapter II of Chapter 53 of Title 31 of the U.S. Code. 18 U.S.C. § 1961(1) references violations of 18 U.S.C. § 1343.

8. 28 U.S.C. § 2461(c) (civil to criminal forfeiture incorporation statute) provides that if a person is charged in a criminal case with a violation for which the civil or criminal forfeiture of property is authorized, the government may include notice of the forfeiture in the charging instrument pursuant to the Rules of Criminal Procedure. If the defendant is convicted of the offense giving rise to forfeiture, the Court shall order forfeiture of the property as part of the defendant's sentence. The procedures of 21 U.S.C. § 853 shall apply to all stages of a criminal forfeiture proceeding, except for subsection (d) of that statute.

9. 18 U.S.C. § 981(b)(3) (civil seizures) provides that notwithstanding the provisions of Fed. R. Crim. P. 41(a), a seizure warrant issued pursuant to that subsection by a judicial officer in any district in which a forfeiture action against the property to be seized may be brought, and may be executed in any district in which the property to be seized is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or international agreement.

10. 21 U.S.C. § 853(f) (criminal seizures) provides that the government may request a seizure warrant authorizing the seizure of property subject to forfeiture in the same manner as for a search warrant. The seizure warrant issues if the Court determines that there is probable cause to believe that the property seized would, in the event of conviction, be subject to forfeiture and that a restraining order may not be sufficient to assure the availability of such property for forfeiture.

11. A restraining order would be inadequate to preserve the two accounts for forfeiture. Based on my training and experience, I know that restraining orders served on banks sometimes fail to preserve the property for forfeiture because the bank representative receiving the restraining order fails to put the necessary safeguards in place to freeze the money in time to prevent the account holder from accessing the funds electronically, or fails to notify the proper personnel as to the existence of the order.

12. Under 18 U.S.C. § 984, for any forfeiture action *in rem* in which the subject property consists of cash, monetary instruments in bearer form, or funds deposited in an account in a financial institution:

- a. The government need not identify the specific funds involved in the offense that serves as the basis for the forfeiture;
- b. It is not a defense that those funds have been removed and replaced by other funds; and
- c. Identical funds found in the same account as those involved in the offense serving as the basis for the forfeiture are subject to forfeiture.

13. In essence, 18 U.S.C. § 984 allows the government to seize for forfeiture identical property found in the same place where the “guilty” property had been kept. The statute does not, however, allow the government to reach back in time for an unlimited period. A forfeiture action (including a seizure) against property not directly traceable to the offense that is the basis for the forfeiture cannot be commenced more than one year from the date of the offense.

**PROBABLE CAUSE**

**THE SCHEME TO DEFRAUD**

14. The FBI, the Treasury Inspector General for Tax Administration (“TIGTA”), and the United States Postal Inspection Service (“USPIS”) (collectively, the “Joint Investigation”), are investigating a conspiracy which exploits the Internal Revenue Service’s (“IRS”) Modernized Internet Employer Identification Number (“Mod IEIN”) online portal. Mod IEIN is the IRS system that allows users to register for a unique Employer Identification Number (“EIN”) for a business. These transactions are processed at IRS Enterprise Computing Centers located in West Virginia and Tennessee, making each of these transactions an interstate wire communication.

15. The investigation shows that Fei LIANG (“LIANG”), Ziguang LI (“LI”), and others obtained EINs for various businesses in furtherance of a scheme to defraud. These EINs allowed the co-conspirators to open business bank accounts<sup>1</sup> at various financial institutions for the purpose of receiving fraudulent wire transfers. Through victim interviews and the review of complaints submitted to the FBI’s Internet Crime Complaint Center (“IC3”),<sup>2</sup> law enforcement has determined that many of these wire transfers were the result of a tech support scam<sup>3</sup> targeting older adults. The proceeds of this fraudulent activity were rapidly withdrawn or moved between bank accounts

---

<sup>1</sup> From training and experience, I know that fraudsters often prefer business bank accounts for schemes involving high dollar transactions. This is due to the perception that banks apply greater scrutiny to large deposits when they are credited to personal bank accounts.

<sup>2</sup> IC3 is an FBI-led program that allows victims of cyber-crime to file formal complaints. These complaints are made available to federal, state, local, or international law enforcement as appropriate.

<sup>3</sup> From training and experience, I know that tech support scams typically involve a fraudster who impersonates an employee of a legitimate technology company (e.g., Microsoft) and offers to “fix” a non-existent problem on the victim’s computer. The fraudster will often trick the victim into (1) giving the fraudster access to the victim’s financial accounts (2) installing malicious software on the victim’s computer, and/or (3) giving the fraudster remote access to the victim’s computer. According to the National Council on Aging’s website “In 2020, at least 66% of tech support scam victims were age 60 or older.”

controlled by different co-conspirators. This rapid movement of funds is indicative of communication and coordination between various individuals in furtherance of the conspiracy.

16. On July 25, 2024, a grand jury indicted LIANG and LI on one count of 18 U.S.C. § 1956(h) (conspiracy to commit money laundering) and six counts of 18.U.S.C. § 1956(a)(1)(B)(i) and 2 (concealment money laundering) (Case No. 1:24-cr-170). It further alleged that the specified unlawful activity is wire fraud, in violation of 18.U.S.C. § 1343 and mail fraud, in violation of 18 U.S.C. § 1341.

#### The Source of Funds: Elder Fraud Scams

17. The investigation revealed a conspiracy that targeted unsuspecting victims through a nationwide tech support scam. Typically, the victims reported receiving a pop-up on their computer. The pop-ups included a phone number to contact for assistance. Once the victims called the phone number, the victim was advised to provide the purported technical support individual access to their computer. Upon doing so, the victim was often informed that their bank account had been hacked and the victim needed to secure their financial assets by transferring their money to the bank accounts associated with the conspiracy. The victim—believing they were sending money to address real issues with their computer and bank accounts—either wired money to bank accounts controlled by LIANG and coconspirators or mailed checks to coconspirators to be deposited into conspirator-controlled bank accounts.

#### The Fictitious Virginia Business Entities

18. On June 16, 2023, Dragon Auto Parts Inc. was incorporated by the Commonwealth of Virginia State Corporation Commission (“SCC”) with a registered agent of B.P. and registered office address of 7630 Little River Turnpike, Ste 720-10, Annandale, Virginia 22003 (“7630 Little

River Turnpike”). 7630 Little River Turnpike is associated with LocalWorks, which is a company that rents office space to individuals and businesses. The investigation revealed that LocalWorks had no records involving B.P. or Dragon Auto Parts Inc. renting office space.

19. On June 21, 2023, TD Bank account number xxxxxx6540 for Dragon Auto Parts Inc. (EIN: 93-1915932) was opened at a location in the Eastern District of Virginia. Included in the TD Bank account opening documents was a Dominion Energy customer bill for an identity theft victim identified here as “B.P.” showing an address of 1515 Richmond Hwy, Unit 906, Arlington, Virginia 22202 (“1515 Richmond Hwy”) dated June 5, 2023.

20. Records from Dominion Energy indicated that they were unable to locate an account associated with B.P., 1515 Richmond Hwy, or the meter number provided in Dominion Energy customer bill. Further, 1515 Richmond Hwy is associated with Crystal Square Apartments. Crystal Square Apartments had no records involving B.P. or Dragon Auto Parts Inc. renting Unit 906 in 2023. I reviewed bank surveillance footage associated with the June 21, 2023 bank account opening for TD Bank xxxxxx6540.

21. Two photographs obtained from the June 21, 2023 TD Bank surveillance footage reviewed are displayed below:



22. I have compared the photographs above with known images of LIANG. Based on that review and my training and experience, I believe the person depicted above to be LIANG.

23. Between June 26, 2023 and July 13, 2023, TD Bank account number xxxxxx6540 was the beneficiary of two wire transfers and one cashier's check deposit totaling over \$139,000. These deposits included a \$39,221.01 wire transfer from Victim-1's M&T Bank account on July 13, 2023. On March 4, 2024, I interviewed a 74-year-old resident of Connecticut (identified here as "Victim-1") who verified that the wire transfer from Victim-1's M&T Bank account to TD Bank xxxxxx6540 was the result of a tech support scam.

24. Further investigation revealed that business bank accounts were opened for Dragon Auto Parts Inc. (using EIN 93-1915932 and B.P.'s identity) at other financial institutions, including PNC, Truist, Citibank, Wells Fargo, and United Bank. Account opening documents associated with the Wells Fargo account in the name of Dragon Auto Parts Inc. indicated the business had five employees and was described as "Tire Shop and Automotive Parts." Financial analysis revealed no deposits or withdrawals consistent with an automotive business.

25. Between June 26, 2023 through October 17, 2023, the bank accounts described

above, all opened in the name of Dragon Auto Parts Inc., were the beneficiary of 19 wire transfers and one cashier's check deposit, totaling over \$670,000, all from known or suspected victims. The FBI interviewed nine additional victims that deposited money into the Dragon Auto bank accounts, all indicating that money transfers were the result of a tech support scam.

26. Based on the fraudulent activity described above, I reviewed the Commonwealth of Virginia SCC records to identify additional businesses located at 7630 Little River Turnpike. This review identified several fictitious businesses, including:

- a. M&M Popular Package Food Inc. (EIN: 93-1572743, registered agent X.W.)
- b. LL Wang Food Trading Inc. (EIN: 93-1571607, registered agent L.W.)
- c. Crysal Accessories Inc. (EIN: 93-1916200, registered agent H.C.)

The investigation has identified each of the businesses referenced above was also associated with the residential address of 1515 Richmond Hwy. LocalWorks and Crystal Square Apartments had no records of the above individuals or entities being associated with their properties.

27. On April 25, 2024, I interviewed X.W., an identity theft victim, whose information was used to incorporate M&M Popular Package Food Inc. X.W. indicated that his identity appeared to have been stolen in the summer of 2023. X.W. filed a police report on July 10, 2023 related to the identity theft. I have compared the photographs of the individual depicted in the M&M Popular Package Food Inc. bank surveillance footage to the individual I interviewed in April 2024 and do not believe the person depicted in the surveillance footage is X.W. I have compared the surveillance footage to known pictures of LIANG. Based on my review, I believe the person depicted in the surveillance footage (purporting to be X.W.) to be LIANG.

28. Upon reviewing various bank records, IRS's Mod IEIN records, Postal Service

Records and the Virginia State Corporation Commission (“SCC”) records, numerous businesses have been identified as being operated by LIANG, LI, and/or other co-conspirators in furtherance of the scheme. The businesses identified include, but are not limited to, the following (collectively the “Fictitious Virginia Business Entities”):

- a. Dragon Auto Parts Inc
- b. M&M Popular Package Food Inc
- c. LL Wang Food Trading Inc
- d. Crystal Accessories Inc
- e. V&L Good Food Wholesale Inc
- f. Dug Duy Food Trading Inc
- g. Coco Love Nail Art Wholesale Inc
- h. Kim Fashionable Clothing Inc
- i. Leslie Cell Phone Accessories
- j. Roger Trucking Service
- k. Above and Beyond Heating Corp
- l. Kunblo Spring City Inc
- m. SZ Façade Management Inc
- n. Universe CCK Computer Inc
- o. Dragon Façade Management
- p. Hong & Yun Clothing Inc
- q. LMH Computer Service Inc
- r. Carson Truck Service Inc

s. Phenix Beauty Supplies Inc

t. Chia Supplies Co Limited

29. On April 30, 2024, a federal search warrant (1-24-SW-304) was issued by the Honorable Magistrate Judge Ivan D. Davis in the Eastern District of Virginia for three devices in LIANG's hotel room. On the cell phone associated with a phone number connected to LIANG, I reviewed WeChat communications between LIANG and coconspirators. The WeChat communications included identification documents, Virginia SCC incorporation documents, utility bills, and financial information associated with many of the Fictitious Virginia Business Entities.

30. To date, I have reviewed over 100 bank accounts associated with the Fictitious Virginia Business Entities. Review of the bank account activity associated with the Fictitious Virginia Business Entities did not identify business income or business expenses. Rather, the bank accounts have nearly no activity other than the receipt of victim funds and the transfer of those funds to related bank accounts, bank accounts linked to other suspected fictitious businesses, and the cash withdrawal of funds. Further, the bank accounts were often only kept open for a couple of months before being closed by the banks.

31. Based on my review of bank surveillance footage, an individual resembling LIANG was depicted conducting financial transactions associated with at least eight different entities, including Dragon Auto Parts Inc, LL Wang Food Trading Inc, Kunblo Spring City Inc, Crystal Accessories, M&M Popular Package Food Inc, SZ Façade Management Inc, Roger Trucking Service Inc, and Kim Fashionable Clothing Inc.

32. Review of the WeChat communications on LIANG's device revealed the exchange

of bank account information, such as passwords and account numbers, associated with many of the Fictitious Virginia Business Entities and bank accounts linked to other suspected fictitious businesses. I believe this was done to facilitate multiple people to access the bank accounts to conduct and review financial transactions. Review of the WeChat communications on LIANG's device also included instructions on which accounts to send money, when to expect victim deposits, and which accounts to deposit victim checks.

#### The Subject Accounts

33. The government has employed the lowest intermediate balance rule ("LIBR") in analyzing the **SUBJECT ACCOUNTS**, meaning the government determined which funds in the respective accounts constitute, or are traceable to, the proceeds of the wire fraud scheme, and which funds are "other funds," *i.e.*, funds not traceable to the wire fraud scheme. LIBR is a method in which the government assumes the "other funds" in a bank account are spent before any funds in the account that constitute or are traceable to the wire fraud scheme. This analysis is strictly based on the categorization of funds and not on the time of deposit; in these analyses, funds derived from a fraud scheme could stay in a bank account for years if the bank account was continually replenished with "other funds" for substantial periods of time.

#### **SUBJECT ACCOUNT 1**

34. On or around August 10, 2023, Carson Truck Service Inc was registered with the Virginia SCC. On or around August 15, 2023, TD Bank account number 4441040807 in the name of Carson Truck Service Inc was opened ("**SUBJECT ACCOUNT 1**"). Prior to August 31, 2023, **SUBJECT ACCOUNT 1** had a balance of \$812.35. Between August 31, 2023 and September 5, 2023, **SUBJECT ACCOUNT 1** received approximately \$149,175 in deposits from three victims,

as detailed below:

- August 31, 2023: \$100,000 from M.P, a 71-year-old residing in Lake Charles, Louisiana;
- September 5, 2023: \$22,875 from P.R., a 67-year-old residing in Philadelphia, Pennsylvania; and
- September 5, 2023: \$20,000 and \$6,300 from S.L., a 77-year-old residing in Glendale, Arizona.

35. All three victims filed IC3 complaints indicating that they were the victim of a tech support scam. There were no other deposits into **SUBJECT ACCOUNT 1**. As of June 30, 2024, the balance of **SUBJECT ACCOUNT 1** was approximately \$22,787. The funds remaining in **SUBJECT ACCOUNT 1** are victim funds and constitute proceeds of mail and wire fraud.

#### **SUBJECT ACCOUNT 2**

36. On or around October 17, 2023, Phenix Beauty Supplies Inc was registered with the Virginia SCC. On or around October 24, 2023, PNC account number 53-6641-9861 in the name of Phenix Beauty Supplies Inc was opened (“**SUBJECT ACCOUNT 2**”). On November 26, 2023, the balance of **SUBJECT ACCOUNT 2** was approximately \$7. Between November 27, 2023 and November 30, 2023, **SUBJECT ACCOUNT 2** received approximately \$70,354 in deposits from three suspected victims, as detailed below:

- November 27, 2023: \$46,000 from M.G., a 78-year-old residing in Mountain View, California;
- November 29, 2023: \$9,854.32 from H.W., a 72-year-old residing in Frederick, Colorado; and
- November 30, 2023: \$14,500 from D.N., a 69-year-old residing in McCormick, South

Carolina.

37. M.G. and H.W. filed IC3 complaints indicating that they were the victim of a tech support scam. Based on my training and experience, I believe that D.N. is also the victim of a tech support scam. During this time period, there were \$6 in additional deposits to **SUBJECT ACCOUNT 2**. As of June 28, 2024, the balance of **SUBJECT ACCOUNT 2** was approximately \$9,358.82. The funds remaining in **SUBJECT ACCOUNT 2** are victim funds and constitute proceeds of mail and wire fraud.

### **SUBJECT ACCOUNT 3**

38. On or around December 19, 2023, Chia Supplies Co Limited was registered with the Virginia SCC. The registered agent is listed as Chia-yu Dennis Liu. On December 7, 2023, LIANG, via WeChat, shared a picture of Liu's Texas driver's license, Liu's date of birth, and Liu's social security number. LIANG requested that a coconspirator run a credit report for Liu. Based on the investigation to date, this activity is consistent with LIANG using another individuals identifying information in order to register a fictitious business open and open bank accounts to receive victim funds.

39. On or around February 1, 2024, Bank of America account number 4350\_4816\_5747 in the name of Chia Supplies Co Limited was opened ("SUBJECT ACCOUNT 3"). On February 1, 2024, **SUBJECT ACCOUNT 3** was opened with a \$100 cash deposit in Dumfries, Virginia. On February 2, 2024, **SUBJECT ACCOUNT 3** received four wire deposits, totaling \$132,842.37, from four suspected victims of a tech support fraud, as detailed below:

- February 2, 2024: \$51,722.37 from S.B., a 69-year-old residing in Oak Ridge, Tennessee;
- February 2, 2024: \$50,000 from J.L., a 75-year-old residing in Meriden, Connecticut;

- February 2, 2024: \$19,700 from L.L., an 80-year-old residing in Washington, D.C.; and
- February 2, 2024: \$11,420 from W.P., a 71-year-old residing in New Kensington, Pennsylvania.

There were no other deposits into **SUBJECT ACCOUNT 3**.

40. On August 19, 2024, I interviewed W.P. who confirmed that they were the victim of a tech support fraud. Based on my training and experience, I believe that S.B., J.L., and L.L. are also victims of a tech support scam.


41. On February 23, 2024, **SUBJECT ACCOUNT 3** was closed and a cashier's check for \$132,882.37 was issued to the customer. As of August 19, 2024, the cashier's check had not yet been cashed and the \$132,882.37 is being held in an internal Bank of America account.

42. On February 5, 2024, in a WeChat group chat<sup>4</sup> involving LIANG and others, including an individual going by "Customs."<sup>5</sup> In the WeChat group "Customs" asked for Chia Supplies Co Limited's Bank of America account information, including the ID used to open the account, associated social security number, and the virtual card number. "Customs" then sent an image of the **SUBJECT ACCOUNT 3**'s online bank account:

---

<sup>4</sup> Review of the WeChat group chat indicated that the individuals involved primarily discussed bank account information associated with the Fictitious Virginia Business Entities, including directions on which accounts to deposit victim funds, where to wire the money once received, and account passwords.

<sup>5</sup> "Customs," associated with WeChat ID wxid\_5z4lkp1etp2212, was observed communicating with LIANG and other coconspirators on when to expect victim deposits, which accounts to direct victim funds be deposited into, and where to send the victim funds once received.

**BANK OF AMERICA**  **Business Advantage 360** Chia Supplies Co Limited | Profile & Settings | Saved Items | Log Out

Accounts | Pay & Transfer | Business Services | Offers & Deals | Tools & Investing | Security Center | Open an Account | Help & Support

**Business Adv Fundamentals - 5747**

**Summary**  
 Available balance (as of today): **\$132,882.37**  
 What does this include?  
 Account balance history »

**Features**  
 Payroll services:  
 Account management:  
 More features »

**Services**  
 Enroll  
 Enroll  
 Scan checks to deposit  
 Order checks/deposit slips  
 Stop payment on a check  
 More services »

Activity | Statements & Documents | Information & Services

**All Transactions** | View Spending & Budgeting

Enter keyword, amount or mm/dd/yyyy | More options

Newest | Next | Previous | Oldest | Download | Print this view

Date	Description	Type	Status	Amount	Available Balance
Processing	HOLD WIRE TRANSFER FEE ON 02/03	⊖	[P]	-15.00	132,882.37
Processing	HOLD WIRE TRANSFER FEE ON 02/03	⊖	[P]	-15.00	132,897.37
Processing	HOLD WIRE TRANSFER FEE ON 02/03	⊖	[P]	-15.00	132,912.37
Processing	HOLD WIRE TRANSFER FEE ON 02/03	⊖	[P]	-15.00	132,927.37
02/02/2024	WIRE TYPE:WIRE IN DATE: 240202 TIME:1558 ET TRN:2024020200502847...	⊕	[C]	11,420.00	132,942.37
02/02/2024	WIRE TYPE:WIRE IN DATE: 240202 TIME:1332 ET TRN:2024020200429762...	⊕	[C]	15,700.00	121,522.37
02/02/2024	WIRE TYPE:WIRE IN DATE: 240202 TIME:1741 ET TRN:2024020200544230...	⊕	[C]	50,000.00	101,822.37
02/02/2024	WIRE TYPE:WIRE IN DATE: 240202 TIME:1418 ET TRN:2024020200452542 SEQ: /001029...	⊕	[C]	51,722.37	51,822.37

**BankAmenDeals®**  
 BankAmenDeals® puts cash back deals right on your cards.  
 Learn more

“Customs” then asked LIANG and conspirators to call Bank of America about **SUBJECT ACCOUNT 3** in order to figure out how to get the money out of the bank account.

43. Based on my training and experience, I have probable cause to believe that the remaining funds held in an internal Bank of America account associated with **SUBJECT ACCOUNT 3** are victim funds and constitute proceeds of mail and wire fraud..

### **CONCLUSION**

44. Based on the facts contained herein, combined with the training and experience of

the investigative team, I conclude that there is probable cause to believe that the **SUBJECT ACCOUNTS** contains the proceeds of wire and mail fraud. The **SUBJECT ACCOUNTS** are therefore subject to seizure and forfeiture pursuant to the statutory authority set forth above.

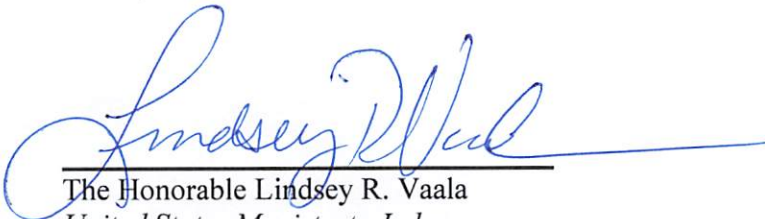
45. Based on the foregoing, it is requested that a seizure warrant be issued for the monies contained within the **SUBJECT ACCOUNTS** identified in this affidavit pursuant to the authority cited above.

Samantha Wendt Digitally signed by Samantha  
Wendt  
Date: 2024.08.22 14:46:34 -0400

---

Samantha Wendt  
Special Agent  
Federal Bureau of Investigation

Attested to me in accordance with the requirements of Fed. R. Crim. P. 4.1 via telephone on August 23 2024.



---

The Honorable Lindsey R. Vaala  
*United States Magistrate Judge*